

MENU

Mobile Security

Data Protection

Identity & Access

CSOM

Oracle WebLogic hackers pick Monero mining over ransomware

Liam Tung (CSO Online) on 12 January, 2018 09:27

0 Comments

5

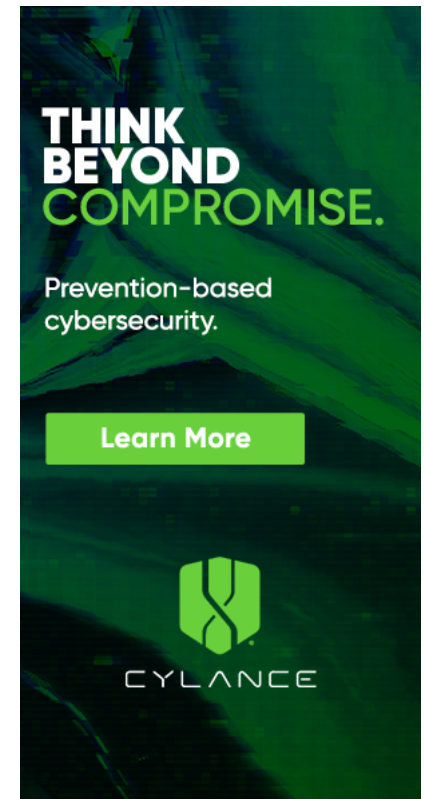


A group of criminals earned nearly \$250,000 by installing a cryptocurrency miner on vulnerable Oracle WebLogic and People Soft servers.

Morphus Labs chief research officer Renato Marinho [reported](#) this week on an uptick in attacks on enterprise servers that exploit a critical WebLogic flaw that [Oracle patched in October](#). But thanks to an exploit published by a Chinese researcher in December, hundreds of un-patched WebLogic and PeopleSoft servers across the globe have been co-opted as mining bots, boosting the attacker's capacity to mine the Bitcoin alternative Monero.

Surprisingly, the WebLogic vulnerability allows the attackers to steal data from affected PeopleSoft systems, or even install ransomware, yet the group so far has only use the vulnerability to install a Monero miner. And it's paying off.

One of the operations using the WebLogic exploit has so far [mined 611 Monero](#) that are worth about \$226,070 currently. The WebLogic exploit helped boost the number of mining bots to work for the attackers, however it's likely many of these Monero were mined prior to December. Another group using the same exploit was mining AEON but had only earned about \$6,000.



Featured Whitepapers



Australia Mandatory Data Breach Notification Report



Using Metrics to Mature Incident Response Capabilities

Editor's Recommendations



Collaboration is key to getting cyber insurance right

Marinho figures the compromised machines were detected because the script that downloads the Monero miner “accidentally” kills the WebLogic service after compromise. WebLogic is a Java EE application server and the script replaces its java binary with the Monero miner xmrig — a legitimate miner that the attackers are illegitimately using on others’ hardware.



More from RSA »

On January 2 an admin [posted](#) a report on Oracle's support forum documenting the same Monero attack after discovering errors that shutdown a WebLogic Service and an Oracle Access Management Server.

Marinho has found hundreds of attacked WebLogic and PeopleSoft servers around the world, which are mostly hosted on cloud services, such as AWS, Digital Ocean, Google, Microsoft, Oracle Cloud and OVH.

In a [follow up analysis](#) Johannes Ullrich, dean of research at the SANS Institute, said the attacks rely on an exploit developed and published by Chinese security researcher Lian Zhang in late December. The vulnerability it targets, CVE-2017-10271, has a CVSS score of 9.8 and is easily exploitable.

“Once the exploit was published, anybody with limited scripting skills was able to participate in taking down WebLogic (/PeopleSoft) servers,” wrote Ullrich.



READ MORE
[Security in the Age of Hybrid Cloud](#)

Both Ullrich and Marinho were surprised the attackers didn't use the exploit to cause more damage, especially given the data hosted on PeopleSoft servers.

“PeopleSoft itself is a complex enterprise process management system. The name implies human resource functions, but the software goes way beyond simple HR features. Typically, “everything” in an organization lives in PeopleSoft,” said Ullrich.

“An attacker would probably have been able to do a lot more damage to an organization by exfiltrating the data that lives on the system, or worse, modify it.”

Read More:

- [Firefox 52 drops Java plugin support, expands HTTP ‘not secure’ warnings](#)
- [Oracle' CPU for January 2017 Facts and figures](#)
- [Small businesses still aren't acting on cybersecurity and most aren't ready for an attack](#)
- [Week in review: How is your Meltdown/Spectre action plan progressing?](#)
- [Maersk took just 10 days to replace 45,000 PCs wiped by NotPetya attack](#)
- [After Oracle WebLogic attacks, Monero mining malware hits Kaseya enterprise users](#)

Join the newsletter!

Or

[Sign in with LinkedIn](#)

[Sign in with Facebook](#)



New year provides enterprises prime opportunity to recalibrate security posture



Online analytics firms leak user passwords from sites

Solution Centres



The Australian Mandatory Data Breach Notification Resource Centre



Stories by Liam Tung



GitHub clobbered by record-breaking 1.35 Tbps 'memcached' DDoS

Fix up patchy smartphone security updates, US warns



'Tiny call, giant reply' junk traffic attacks aided by 100,000 vulnerable servers



Online analytics firms leak user passwords from sites

Latest Videos



Hunting for Hackers - Why Preventive Measures are Only Part of the Cyber Solution, Duncan Alderson, Senior Manager, Cyber & Forensics, PwC Australia | IDG Security Day

Hunting for Hackers - Why Preventive Measures are Only Part of the Cyber Solution, Duncan Alderson, Senior Manager, Cyber & Forensics,

CSO WANTED

Have an opinion on security? Want to have your articles published on CSO? Please contact CSO Content Manager for our guidelines.

PwC Australia | IDG Security Day

▶ PLAY VIDEO

- Tags
- Oracle
- ransomware
- WebLogic
- cyber security
- peoplesoft
- SANS Institute's Internet Storm Centre
- More about
- AEON
- AWS
- Google
- Home
- Microsoft
- Oracle
- PeopleSoft
- SANS Institute

Read next



10 steps to take ahead of Australia's new data breach regulations



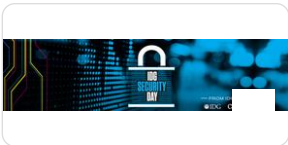
Cisco bug lets anyone login to network as admin with a blank ...



Grappling with DevOps Security



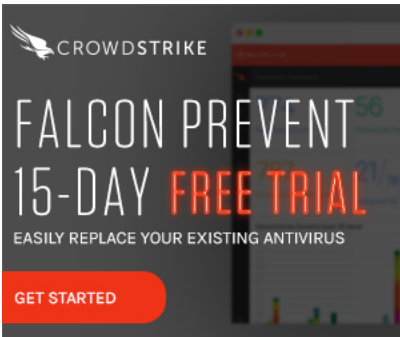
In Pictures: ZertoCON 2017 Sydney



IDG Security Day: Sydney infosec leaders



Cybersecurity Insights - People



0 Comments CSO Australia

1 Login

Recommend Share

Sort by Best

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

Be the first to comment.

Subscribe Add Disqus to your siteAdd DisqusAdd Privacy



Interview with David Sykes, Business Leader, Sophos | IDG Security Day

Interview with David Sykes, Business Leader, Sophos | IDG Security Day

▶ PLAY VIDEO



Showreel | IDG Security Day conference, 21st June

Showreel | IDG Security Day conference, 21st June

▶ PLAY VIDEO



Tools of the Trade: A Live Hacking Demonstration - Ty Miller, Director, Threat Intelligence | IDG Security Day

Tools of the Trade: A Live Hacking Demonstration - Ty Miller, Director, Threat Intelligence | IDG Security Day

▶ PLAY VIDEO



Publisher's Panel - Using AI for next-generation Cyber Security | IDG Security Day

Publisher's Panel - Using AI for next-generation Cyber Security | IDG Security Day

▶ PLAY VIDEO

More videos

Blog Posts

Top 3 Targeted CyberAttacks in 2017

Paul Colmer

Check out the really important new feature of the iPhone application in Gmail

Ritesh Mehta

Are all proxies actually security assets?

Matthew Hackling

Awareness

Matt Tett



[Send Us E-mail](#) | [Privacy Policy \[Updated 23 May 17\]](#) | [Subscribe to emails](#) | [Contacts](#)

Copyright 2018 IDG Communications. ABN 14 001 592 650. All rights reserved. Reproduction in whole or in part in any form or medium without express written permission of IDG Communications is prohibited.

IDG Sites: [PC World](#) | [GoodGearGuide](#) | [Computerworld Australia](#) | [CIO](#) | [CMO](#) | [Techworld](#) | [ARN](#) | [CIO Executive](#)